TechNotes

ITEA Journal 2010; 31: 316–320

Real-Time Targeting for Network Enabled Weapons

Scott R. Frame
46th Test Wing, Eglin Air Force Base, Florida

The continual movement within the Department of Defense to advance net-centric warfare capabilities in operational environments has presented new challenges for test and evaluation of network enabled weapons. The Network Enabled Weapon Real-Time Targeting Tool (NEWRTTT), developed by the 46th Test Wing at Eglin Air Force Base, was created to combine real-time time-space-position information (TSPI) with user-specified test parameters into a targeting message that can be relayed to a network enabled weapon. NEWRTTT receives TSPI data sent from an instrumented dynamic target and uses it along with user-specified test parameters to build an In-Flight Target Update (IFTU). IFTUs are constructed as Link 16 messages, which are packaged using the Joint Range Extension Application Protocol (JREAP) and injected into the net-centric environment using a Link 16 gateway. Latency errors can be injected by the test engineer to evaluate the tolerance of the network enabled weapon under test. Extensibility of TSPI formats is achieved with a well-defined software interface for adding new TSPI sources. Adherence to Department of Defense standard protocols (Link 16, JREAP-C) makes NEWRTTT capable of supporting test and evaluation activities for any Link 16–capable network enabled weapon.

Key words: Dynamic targets, targetting system accuracy; developmental test; operational test; live, virtual, constructive environments; real-time test capability; uncertainty.

As weapon systems advance in sophistication and complexity, the tools and infrastructure of the test and evaluation (T&E) community must also evolve. Operational and test systems can often be adapted to the needs of the changing landscape, but this can lead to monolithic systems with spiraling scope and ever-increasing maintenance requirements. In addition, when operational concepts change dramatically, adaptation of existing systems is no longer feasible, and new approaches must be considered. The advent of network enabled weapons and recent advances in weapon capability have established a need for new test methods and capabilities commensurate with burgeoning netcentric weapon systems (Caravello, Pearce, and Estep 2007).

The operational concept of engaging dynamic targets (moving, mobile, or fixed) by providing weapon directives to a network enabled weapon while it is in flight is depicted in *Figure 1*. A typical scenario for a network enabled weapon engagement involves a targeting source, a launch aircraft, and the network enabled weapon itself. Operationally, the targeting source would likely be sent from a Joint Terminal Attack Controller (JTAC), on the ground, identifying a nearby target. In the corresponding test scenario, this is not a preferred solution; not only would there be concerns with safety, but there would be distinct limits to the levels of variance and error injection that could be applied to the test.

A more desirable test solution involves remote operation and instrumentation of ground targets, which allows operators to remain at safe distances well outside the weapon footprint and eliminates the need for JTAC support *(Figure 2)*. This solution also allows the test engineer to inject more engineering rigor into the test scenario by varying latencies and other test parameters. Target vehicles are instrumented with positioning equipment that renders ground truth time-space-position information (TSPI) and reports it to a test facility over existing T&E infrastructure. This TSPI data must be decoded and then used to build targeting messages for the weapon; once the targeting messages are built, they are submitted for entry onto the network and forwarded to the weapon. Ideally the fields and specifications for sending the targeting messages can be manipulated as the messages are being sent to vary test parameters in accordance with

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Real-Time Targeting for Network Enabled Weapons	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **46th Test Wing,Eglin AFB,FL,32542**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**5**	

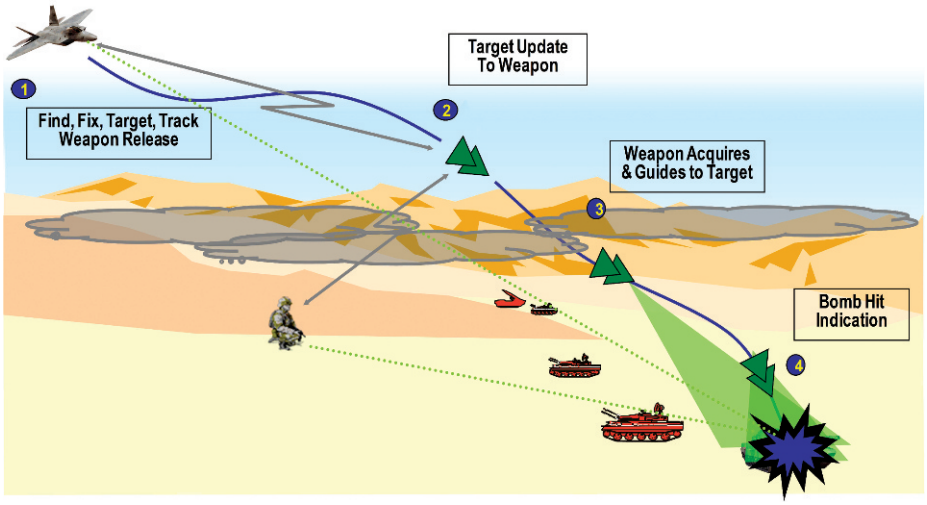

Figure 1. Network enabled weapon concept of operations.

threshold and objective goals for the system under test. Another benefit to this type of configuration is that the ground truth TSPI data can be used for comparison with an operational targeting source. This accommodates another test scenario in which it is possible to evaluate the accuracy of a targeting system rather than the accuracy of a weapon.

Considerations for real-time targeting

Effective T&E of network enabled weapons requires a test solution for the real-time targeting of these weapons. For developmental testing in particular, it is essential to find a safe way to relay precise target information from a dynamic test target. Any implementation of such a solution should be able to accept precision TSPI from instrumented targets over existing T&E infrastructure and to produce the necessary targeting message for submission into the net-centric environment. Test parameters for error injection and track/target management should be configurable by the test engineer. The operational environment contains inherent uncertainties and latencies; the test environment should be able to operate with or without these variables, and the level of variability should be selectable by the test engineer. The ability to eliminate and control uncertainty is essential for effective testing. For posttest analysis, the ability to capture and either log or playback processed data would give the test solution increased capability.

Because of increasing focus on live, virtual, and constructive (LVC) methods in recent years, applicability of a real-time targeting solution for network enabled weapons to LVC environments is an important capability. The LVC environment provides testers

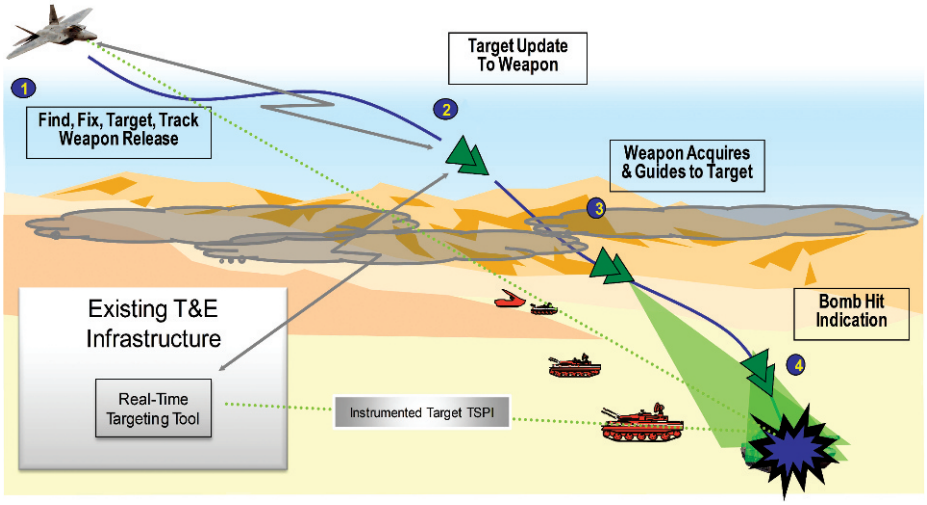

Figure 2. Network enabled weapon test scenario.

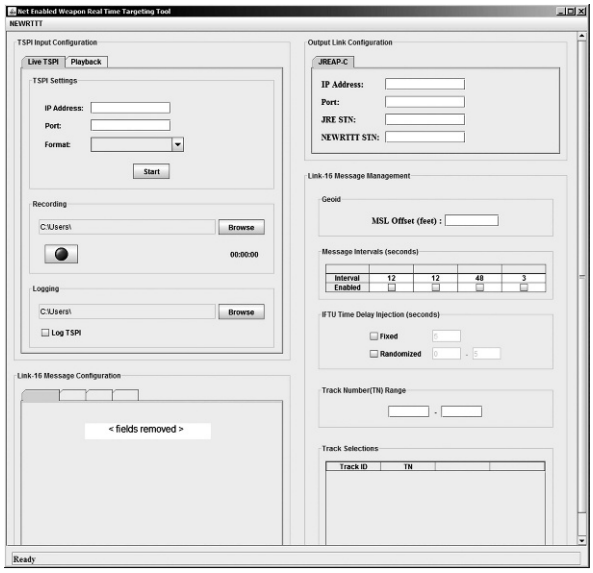

Figure 3. Network enabled weapon real-time targeting tool application screen capture.

with the opportunity to test a system of systems in ways that are not possible during a strictly live test; precise environmental control, low-cost iterated test runs, and load-testing of systems make LVC testing an invaluable supplement to more traditional forms of testing. A suitable network enabled weapon test solution should be able to participate in the reception of TSPI input tracks from LVC domains and inject targeting messages into the LVC domain. Record and playback features have particular importance in the LVC environment, since a simulated event can be recorded or fabricated and then used as desired for subsequent events.

Network Enabled Weapon Real-Time Targeting Tool (NEWRTTT)

The NEWRTTT was created to provide a real-time test capability for network enabled weapons. It is a pure software solution to network enabled weapon testing requirements for real-time systems that works in coordination with the existing T&E infrastructure to achieve net-centric warfare test objectives. A screen capture of the NEWRTTT application is displayed in *Figure 3*. TSPI data received from instrumented dynamic targets on a test range are injected into the tool; these data are decoded, converted, and supplemented with operator-supplied test parameters, and a targeting message is constructed for dispatch to a network enabled weapon. Targeting updates are constructed as Link 16 messages that are packaged using the Joint Range Extension Application Protocol (JREAP). These messages are output to a Link 16 gateway, which injects them onto a Link 16 network.

Because NEWRTTT was created to work within the existing T&E network infrastructure, the input interface was designed to be modular and flexible. NEWRTTT accepts TSPI input using standard User Datagram Protocol (UDP) network sockets. TSPI input settings are configured on the user interface. The format of the TSPI data is selectable and allows for extensibility of TSPI formats. This is an important feature with regards to the portability of NEWRTTT, since many T&E labs and facilities exist and often they deal with a variety of TSPI formats.

The output interface requires adherence to specific Department of Defense (DoD) standards that implement the targeting message for network enabled weapons. The targeting message is referred to as an in-flight target update (IFTU) and is part of a new series of messages that allow coordination and control of network enabled weapons using the Link 16 data link to implement the communication. Though the specification is not finalized and still subject to change, some C2 and weapons systems are already implementing the new messages.

Crafted Link 16 IFTU messages, by themselves, are not suitable for transmission over an Internet Protocol (IP)-based network; they must be wrapped inside another transmission protocol that provides additional information about the message originator, destination, size, time, etc. NEWRTTT currently implements the JREAP-C standard for transmitting output messages to a Link 16 gateway. The JREAP-C packets are constructed and sent to a Joint Range Extension—a gateway that hosts a Link 16 terminal and has the ability to inject messages onto a Link 16 network. In addition to the JREAP-C capability, another transport protocol, Multi-TADIL capability, will be added to NEWRTTT in a future increment.

Extensibility of TSPI formats

One initial and key goal for NEWRTTT was portability. Portability allows the tool to be used on a variety of systems in diverse environments and to provide a useful test capability to any major range and test facility base. Test platforms may consist of large-scale test facilities with extensive T&E infrastructure, distributed LVC environments, training facilities or even a laptop connected to C2 equipment in a van out on a test range. The difficulty in achieving portability in all of these settings lies in creating a solution that is flexible enough to accommodate the extensive variety of test systems and TSPI data formats. The Java programming language was chosen to achieve platform independence, allowing the application to run on any machine with a current Java Virtual Machine. This made the variety of TSPI inputs the constraining factor

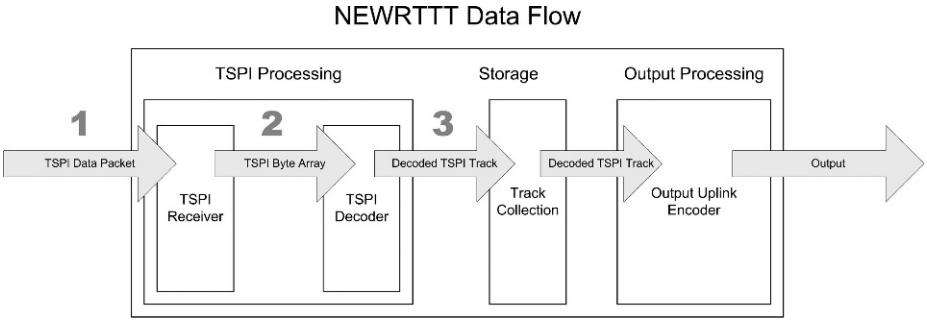

Figure 4. Standard time-space-position information processing data flow.

for achieving portability. Some test facilities may use systems that adhere to known TSPI standards, while others may use proprietary protocols that are only useful at a single site. Even if only standard TSPI formats were used, there is such an abundance of these formats that accounting for all of them is not feasible. To overcome this hurdle, NEWRTTT was equipped with a well-defined, thoroughly documented interface for incorporating new TSPI decoders into the tool. *Figure 4* depicts the standard TSPI processing data flow through the application.

The processing of incoming TSPI data in the NEWRTTT consists of three steps:

1. Read TSPI data from a network.
2. Decode the received TSPI data using an appropriate data decoder.
3. Store the decoded TSPI data into a collection of TSPI tracks.

To add a new TSPI decoding capability, a single Java class file can be written that decodes the fields of the TSPI data and reports them to the main program. The interface involves steps 2 and 3 of the NEWRTTT Data Flow, as depicted in *Figure 5*. It allows a decoder developer to create a single Java class that implements the decoding routine to (a) decode the data into a standard format, and (b) store the data into a collection. When creating the decoder, the developer must implement a specific interface for the decoding class.

Message management

NEWRTTT allows the tester precise control over messages to be output. In addition to the IFTU message, NEWRTTT also allows the tester to output surveillance and precise participant location and information messages. NEWRTTT incorporates features to manage these messages in three ways:

1. message field configuration,
2. transmission control,
3. simulated/controlled error injection.

Message field configuration allows non-TSPI fields of the output messages to be manipulated by the operator. Though much of the data used to populate the output messages come from the input TSPI, many fields of the output are not TSPI specific. Some of

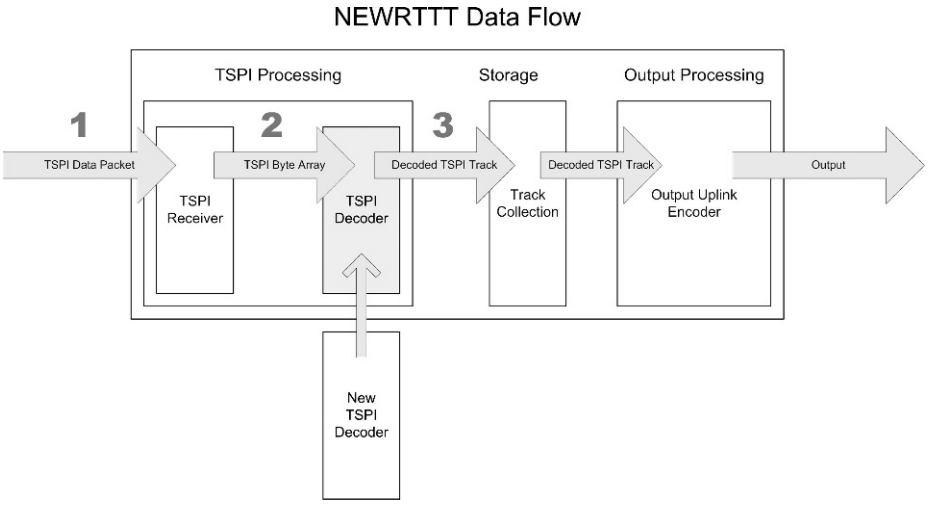

Figure 5. Insertion of time-space-position information decoder.

these fields can be set permanently for the tool because of the nature of the application, but others may need to be set by the test engineer to allow for flexibility. NEWRTTT provides the test engineer the ability to configure these fields.

Transmission control of messages is managed on a type level and a track level. Each message type is controlled independently, so that messages can be enabled or disabled, or the output rate can be adjusted as necessary. For IFTU messages and surveillance messages, output message designations are selected on a per-track basis. Multiple surveillance tracks can be sent out simultaneously, but only a single track can be selected for IFTUs at a given time. When TSPI data are processed, the track IDs for any successfully decoded TSPI tracks are used to populate a table of available tracks. Link 16 track number reference assignments are selected from a pool of available track numbers and given to each decoded TSPI track. These track number assignments can be reassigned manually by the tester, providing additional control of track management.

One important goal of NEWRTTT is to provide the capability to inject simulated or controlled errors. Time delay errors can be injected into IFTU messages as specified by the tester. The tool provides an option to inject a fixed time delay or a randomized time delay. IFTU messages are prepared at the normal output rate, but when the time to send them arrives, transmission is deferred until the assigned delay has expired. Future enhancements will incorporate target location error as another source of injected error, which will allow for more controlled variation of the test environment.

Conclusions

A number of network enabled weapon systems are quickly approaching phases of extensive T&E. Because of DoD direction to standardize technologies and communication protocols, many of these tools will conform to common interfaces and have similar applications. The capabilities of network enabled weapons and the supporting infrastructure have only recently begun to take form, and the testing of these systems of systems will involve a combination of new open air methods and innovative LVC approaches. The NEWRTTT provides a means to tackle some of the challenges of this new and complex test environment. It is applicable to both developmental and operational test and will evolve with the needs of the net-centric warfare community to support T&E for a variety of network enabled weapons. Future development increments are already in discussion to extend the IFTU capability, incorporate more input formats (including TENA—the Test and Training Enabling Architecture), add the multi-TADIL capability as an alternative to JREAP-C, and support other types of error injection. As the operational concepts of net-centric warfare evolve, the weapon systems and technologies will also change rapidly. NEWRTTT provides a solution to a gap in existing T&E infrastructure that has recently developed as a result of these changes. ❑

Scott R. Frame is a computer engineer for the 46th Test Wing at Eglin Air Force Base, where he develops real-time software applications for munitions testing and situational awareness. He has worked for the Department of Defense for over 6 years, as a computer and software engineer for the U.S. Navy and Air Force. Notable experience includes research and development on the Navy Critical Area Protection System (CAPS) and the U.S. Marines Expeditionary Fighting Vehicle (EFV). He received bachelor of science degrees in electrical engineering and computer engineering from the University of Florida and is currently pursuing a master of science degree in computer science from the University of West Florida. E-mail: scott.frame@eglin.af.mil

References

Caravello, C., S. D. Pearce, and J. A. Estep. 2007. Net-enabled weapons test and evaluation using live, virtual, and constructive methods. In *U.S. Air Force T&E Days*. AIAA-2007-1609, February 2007, Destin, FL. Reston, VA: American Institute of Aeronautics and Astronautics.